

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2002-290418
(P2002-290418A)

(43) 公開日 平成14年10月4日 (2002.10.4)

(51) Int.Cl. ⁷	識別記号	F I	テ-マ-ト* (参考)
H 0 4 L 12/28	3 0 0 1 0 0	H 0 4 L 12/28	3 0 0 Z 5 J 1 0 4 1 0 0 H 5 K 0 3 2
H 0 4 B 3/54		H 0 4 B 3/54	5 K 0 3 3
H 0 4 L 9/08		H 0 4 L 12/40	Z 5 K 0 4 6
9/18		9/00	6 0 1 C
審査請求 有 請求項の数10 O L (全 12 頁) 最終頁に続く			

(21) 出願番号 特願2001-90070(P2001-90070)

(22) 出願日 平成13年3月27日 (2001.3.27)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 大喜多 秀紀

神奈川県横浜市磯子区新杉田町8番地 株
式会社東芝横浜事業所内

(72) 発明者 山田寺 真司

神奈川県横浜市磯子区新杉田町8番地 株
式会社東芝横浜事業所内

(74) 代理人 100083161

弁理士 外川 英明

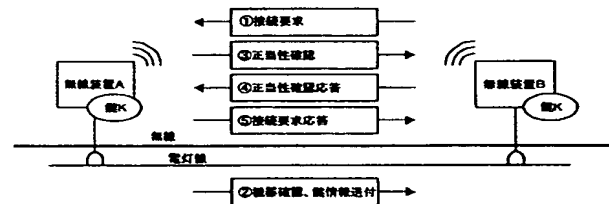
最終頁に続く

(54) 【発明の名称】 無線装置

(57) 【要約】

【課題】従来の無線装置による接続では、高セキュリティやプラグアンドプレイ接続機能を必要とする無線1394によるデジタル映像コンテンツの伝送には適用できない。

【解決手段】無線装置Bから無線装置Aに対し接続要求を送信する。次に無線装置Aから無線装置Bに対して電灯線（有線）経由で鍵情報（鍵K）を送付する。無線装置Aは接続要求装置の正当性を確認する。無線装置Bは正当性確認に応答する。正当性を確認した無線装置Aは接続要求が受理されたことを無線装置Bに通知し、これによりデータ通信が行われる。



【特許請求の範囲】

【請求項 1】 無線通信手段および有線通信手段を有し、他の無線装置と無線により通信する無線装置であって、前記無線通信手段で他の無線装置と無線によるデータ通信をする前に、前記有線通信手段を介して前記他の無線装置と通信可能か否かに応じて無線通信するか否かを決定することを特徴とする無線装置。

【請求項 2】 無線通信手段および有線通信手段を有し、他の無線装置と無線により通信する無線装置であって、前記無線通信手段により他の無線装置と無線によるデータ通信をする前に、前記有線通信手段を介して前記他の無線装置の存在を、前記有線通信手段を用いて確認する手段と、

前記有線通信手段により前記他の無線装置の存在が確認できたとき、装置を識別するための情報である装置識別情報を前記有線通信手段により前記他の無線装置に送信する手段と、前記他の無線装置が前記装置識別情報を保有しているか否かを前記無線通信手段を用いて確認する確認手段と、前記確認手段による確認の結果、前記他の無線装置が前記装置識別情報を保有していることが確認できたとき前記他の無線装置と無線によるデータ通信を許可し、確認できないとき前記他の無線装置と無線によるデータ通信を許可しない制御手段を備えたことを特徴とする無線装置。

【請求項 3】 無線通信手段および有線通信手段を有し、他の無線装置と無線により通信する無線装置であって、前記無線通信手段で他の無線装置と無線通信する前に、前記有線通信手段を介した前記他の無線装置の存在確認要求に回答する存在確認応答手段と、前記無線通信手段で前記他の無線装置と無線通信する前に、前記他の無線装置から装置を識別するための情報である装置識別情報を、前記有線通信手段を介して受信する装置識別情報受信手段と、前記他の無線装置からの前記無線通信手段を介した前記装置識別情報の保有確認に回答する装置識別情報応答手段と、前記他の無線装置による無線によるデータ通信を許可するか否かの判断結果に応じて前記他の無線装置と無線によるデータ通信を行う制御手段とを備えたことを特徴とする無線装置。

【請求項 4】 無線通信手段および有線通信手段を有し、他の無線装置と無線により通信する無線装置であって、前記無線通信手段により他の無線装置と無線によるデータ通信をする前に、前記有線通信手段を介して前記他の無線装置にスクランブル鍵情報を送信するスクランブル

鍵情報送信手段と、

前記無線通信手段により前記他の無線装置と無線によるデータ通信をする前に、前記無線通信手段を介して前記他の無線装置に所定のデータを送信する所定データ送信手段と、

前記他の無線装置から送られてきた、前記所定のデータを前記スクランブル鍵情報により暗号化した暗号化データを受信する暗号化データ受信手段と、

前記暗号化データを前記送信したスクランブル鍵情報に応じたデスクランブル鍵情報により復号化する復号化手段と、

前記他の無線装置に送信した前記所定のデータおよび前記復号化手段により復号化されたデータが同じか否かを判定する判定手段と、

前記判定手段の判定結果が同じと判定されたときに前記無線通信手段を介して前記他の無線装置と無線によるデータ通信を許可し、同じでないと判定したときに前記無線通信手段を介して前記他の無線装置との無線によるデータ通信を許可しない制御手段とを備えたことを特徴とする無線装置。

【請求項 5】 無線通信手段および有線通信手段を有し、他の無線装置と無線により通信する無線装置であって、

前記無線通信手段で他の無線装置と無線によるデータ通信をする前に、前記有線通信手段を介して前記他の無線装置からスクランブル鍵情報を受信するスクランブル鍵情報受信手段と、

前記無線通信手段で前記他の無線装置と無線によるデータ通信をする前に、前記無線通信手段を介して入力された所定のデータを受信する所定データ受信手段と、

前記所定のデータを前記スクランブル鍵情報により暗号化した暗号化データを、前記他の無線装置へ送信する暗号化データ送信手段と、

前記他の無線装置が前記暗号化データを受信し判定した結果に応じて、前記無線通信手段を介して前記他の無線装置と無線によるデータ通信を制御する制御手段とを備えたことを特徴とする無線装置。

【請求項 6】 前記スクランブル鍵情報を記憶する記憶手段を有し、

前記暗号化データ送信手段は、前記有線通信手段が有線接続されていない状態でも、前記無線通信手段を介して入力された前記所定のデータを前記記憶手段に記憶されている前記スクランブル鍵情報により暗号化した暗号化データを前記他の無線装置へ送信することを特徴とする請求項 5 に記載の無線装置。

【請求項 7】 前記装置識別情報は、データ暗号化のための鍵情報であることを特徴とする請求項 2 または 3 に記載の無線装置。

【請求項 8】 前記装置識別情報は、無線通信のための設定情報であることを特徴とする請求項 2 または 3 に記

載の無線装置。

【請求項 9】 前記有線通信手段は、電灯線または有線の IEEE 1394 ネットワークであることを特徴とする請求項 2、3、5、6 のいずれか 1 項に記載の無線装置。

【請求項 10】 前記有線通信手段は電灯線に接続されており、この電灯線は家庭内の別の電灯線に情報を転送するブレーカ装置を含むことを特徴とする請求項 2、3、5、6 のいずれか 1 項に記載の無線装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、ネットワーク接続される装置に関し、特に無線によりネットワークに接続される装置に関する。

【0002】

【従来の技術】従来、無線装置において無線経由でアクセス要求があった場合、家庭内の装置と隣接する家に設置されている外部の装置とを区別する手段が無いため、外部から不正にアクセスされる問題がある。これに対し装置毎に暗証番号等の装置識別情報を入手で設定し区別する手段が考えられるが、装置台数が多い場合や装置操作に不慣れな利用者には適用しにくいという問題があった。

【0003】これら暗証番号を用いた無線装置については、例えば特開平 11-146452 号公報に開示されている。この公報に開示されている技術では、登録子機にそれぞれ暗証番号を設定しておき、該登録子機から ID 情報を取得することで外部からの不正な登録でないかを区別し、新規登録子機の設定を簡便に行うものである。詳細には、子機側からモード設定可能な子機登録方式を得るため子機間通信モードにする。暗証番号と電話番号を利用し、子機 2、3 を通信状態とする。新規登録子機 3 は既登録子機 2 に格納されている親機の ID 情報のコピー要求すると、既登録子機 2 は親機 1 の ID 情報を送出する。新規登録子機 3 は既登録子機 2 からの親機 ID 情報を記憶する。子機 3 が親機の電波到達範囲内に来たとき親機 ID 情報を受信し、子機 2 からコピーした ID 情報と比較して一致した場合には子機登録の要求を行う。親機は子機 3 との子機登録動作を自動的に開始し、子機登録を行う。

【0004】しかし、この従来技術では、親機および全ての子機に対し 1 度は暗証番号を設定しなければならず、装置台数が多い場合作業が大変になる。更に暗証番号は入手で入力する必要があるため、映像コンテンツの伝送等コピー制御を含む高セキュリティを要求される分野には適用しにくい。例えば従来の装置における暗証番号等装置識別用の ID は 4 桁の数字等人が入力可能な短いものが一般的であり、セキュリティレベルが低く、高いセキュリティレベルを要求されるデータの伝送には不向きであった。例えば DVHS や DVD やデジタル放送

等のデジタル映像コンテンツでは、コンテンツの著作権保護（不正コピー防止）が必要不可欠であり、高いセキュリティレベルが必要である。

【0005】家庭用 AV 装置でのデジタル映像コンテンツの伝送に用いられる IEEE 1394 では、DTC P (Digital Transmission Content Protection) というコピー保護手段をこのコンテンツ保護のために用いる。これは各装置が公的な認証機関が発行する鍵を用いた認証により、正しく認証機関からライセンスを受けた装置同士でデジタル映像コンテンツの伝送を行う手段である。このため不正ライセンス装置にデジタル映像コンテンツが不正に流出することを防いでいる。設定なしに接続しただけで動作するプラグアンドプレイ機能を持つ IEEE 1394 では、ライセンス装置同士であれば、デジタル映像コンテンツの伝送が可能である。有線の IEEE 1394 では、接続は家庭内の装置としか接続されていないことが容易にわかるので、プラグアンドプレイによる接続で何ら問題は生じない。

【0006】しかしながらプラグアンドプレイ（設定なしにつながだけで動作する）による接続を前提とした IEEE 1394 を無線に拡張した無線 1394 (Wireless 1394) では、接続のための設定を省く必要があるため上記公報に記載された技術は適用することができず、家庭内の装置へ隣の家等から無線でプラグアンドプレイ接続することができてしまうという問題がある。

【0007】

【発明が解決しようとする課題】このように従来の無線装置による接続では、従来簡単な暗証番号を個々の装置に設定することで装置登録を行っており、高セキュリティやプラグアンドプレイ接続機能を必要とする無線 1394 によるデジタル映像コンテンツの伝送には適用できないという問題があった。

【0008】この発明は、特にプラグアンドプレイを前提とする無線装置間の接続時において、人手による設定を行わずに隣接した家等外部からの不正な接続要求を排除し、同一家庭内の装置のみの安全な無線通信ネットワークを構築することを目的とする。

【0009】また、この発明は冗長な設定なしに同一家庭内装置のみが知り得る暗号鍵を用いて、データを暗号化通信し、外部からのデータ盗聴を防ぐことを目的とする。

【0010】

【課題を解決するための手段】上記の目的を達成するために、この発明においては、無線通信手段および有線通信手段を有し、他の無線装置と無線により通信する無線装置であって、前記無線通信手段で他の無線装置と無線によるデータ通信をする前に、前記有線通信手段を介して前記他の無線装置と通信可能か否かに応じて無線通信するか否かを決定することを特徴とする無線装置を提供する。

【0011】また、無線通信手段および有線通信手段を有し、他の無線装置と無線により通信する無線装置であって、前記無線通信手段により他の無線装置と無線によるデータ通信をする前に、前記有線通信手段を介して前記他の無線装置の存在を、前記有線通信手段を用いて確認する手段と、前記有線通信手段により前記他の無線装置の存在が確認できたとき、装置を識別するための情報である装置識別情報を前記有線通信手段により前記他の無線装置に送信する手段と、前記他の無線装置が前記装置識別情報を保有しているか否かを前記無線通信手段を用いて確認する確認手段と、前記確認手段による確認の結果、前記他の無線装置が前記装置識別情報を保有していることが確認できたとき前記他の無線装置と無線によるデータ通信を許可し、確認できないとき前記他の無線装置と無線によるデータ通信を許可しない制御手段を備えたことを特徴とする無線装置を提供する。

【0012】また、無線通信手段および有線通信手段を有し、他の無線装置と無線により通信する無線装置であって、前記無線通信手段で他の無線装置と無線通信する前に、前記有線通信手段を介した前記他の無線装置の存在確認要求に応答する存在確認応答手段と、前記無線通信手段で前記他の無線装置と無線通信する前に、前記他の無線装置から装置を識別するための情報である装置識別情報を、前記有線通信手段を介して受信する装置識別情報受信手段と、前記他の無線装置からの前記無線通信手段を介した前記装置識別情報の保有確認に応答する装置識別情報応答手段と、前記他の無線装置による無線によるデータ通信を許可するか否かの判断結果に応じて前記他の無線装置と無線によるデータ通信を行う制御手段とを備えたことを特徴とする無線装置を提供する。

【0013】

【発明の実施の形態】（接続要求に応答する無線装置の構成）以下、本発明の実施の形態を図面を用いて詳細に説明する。

【0014】図1は、本発明に係る接続要求に応答する無線装置の構成を説明するためのブロック図である。

【0015】この無線装置は他の無線装置からの接続要求に対して、家庭内の無線装置からの接続であるかを確認し、安全に接続を確立する接続要求応答装置に関するものである。

【0016】まず、無線装置100の構成について説明する。

【0017】図1に示すように、無線装置100は、他の機器と無線により通信を行う無線通信部101、他の無線装置からの接続要求に応答する接続要求応答部102、他の無線装置が家庭内に存在するか否かを確認する無線装置存在確認部103、無線通信部101を介して他の無線装置の正当性を確認する正当性確認部104、スクランブルに用いる鍵情報を管理する鍵情報管理部105、無線通信部101とは別の系（例えば有線）で通

信を行う第2通信部106、通信するデータを暗号化・復号化する暗号化・復号化部107、通信するデータを送受処理するデータ処理部108から構成されている。

【0018】次に、このように構成された無線装置100の動作について詳細に説明する。

【0019】無線通信部101は、他の無線装置から受信した接続要求を接続要求応答部102に出力する。

【0020】接続要求応答部102は、無線通信部101から接続要求が入力されると、通信に用いるID情報を無線装置存在確認部103に出力する。この通信に用いるID情報の具体例としては装置固有のMACアドレスや、IEEE1394で用いられるノードID、エコーネット規格で定義されるエコーネットアドレス等がある。なお通信に用いるID情報は本発明の示す鍵情報等の装置識別情報とは別のものである。

【0021】通信に用いるID情報はプラグアンドプレイ接続により設定なしに装置間で通信を行うために伝送されるものであるが、このID情報だけでは家庭内の装置であるか外部からのアクセスであるかを区別することはできない。家庭内装置からのアクセスを外部からの不正アクセスから区別するためには通信に用いるID情報とは別の装置識別情報が必要となる。

【0022】無線装置存在確認部103は、接続要求応答部102から入力された通信に用いるID情報を基に、第2通信部106を通じて、前記接続要求を出した他の無線装置の存在を確認する。

【0023】第2通信部106の具体例としては、エコーネット等で通信に用いる電灯線やIEEE1394の無線拡張である無線1394がある。

【0024】無線装置存在確認部103は、第2通信部106が前記接続要求を出した他の無線装置の存在を確認できた場合、この確認結果を鍵情報管理部105に出力する。

【0025】鍵情報管理部105は、管理していた鍵情報を正当性確認部104へ出力すると共に、管理していた鍵情報を第2通信部106を経由して上記存在を確認した無線装置に出力する。本実施の形態では装置識別情報として鍵情報を用いた例を示している。鍵情報の具体例としては無線LANで用いられるWEP鍵情報等がある。WEP鍵情報は128bitの長さをもつ鍵情報である。また装置識別情報として無線接続のための設定情報を用いることもできる。

【0026】無線接続のための設定情報の具体例としてはチャンネルやESS-ID等がある。無線接続手段としてIEEE802.11bやIEEE802.11aで規定される無線LANを用いる場合、個々の装置毎にチャンネルやESS-IDを設定する必要がある。この場合、接続要求装置は第2通信部106を経由して接続要求を行い、設定情報を接続要求装置から取得することで、第2通信部106により接続するだけで無線通信を

開始することが出来るようになる。なお無線通信の具体例としては他に無線1.394やBLUETOOTHがある。無線通信の手段毎に接続方法や初期設定の有無等は異なり、無線接続の方法は本実施例の限りではない。

【0027】正当性確認部104は正しい無線装置（家庭内の無線装置）に鍵情報が通知されたかを無線通信部101を経由して確認する。正当性確認の具体的な方法としては公開鍵暗号方式として一般に知られている2パス相手認証やメッセージ認証等の手法が利用できる。

【0028】接続要求した他の無線装置が正しい無線装置（家庭内の無線装置）の場合、正当性確認部104は、無線通信部101を経由して前記接続要求を出した他の無線装置の正当性を確認した（家庭内の無線装置であることが確認できた）ことを接続要求応答部102へ出力する。すると接続要求応答部102は、接続要求を受理したことを示す接続要求受理信号を無線通信部101を介して他の無線装置へ出力すると共に、無線装置存在確認部103を介して鍵情報管理部105へも出力する。

【0029】反対に、接続要求した他の無線装置が正しくない無線装置（家庭内の無線装置でない）の場合、正当性確認部104は、無線通信部101を経由して前記接続要求を出した他の無線装置の正当性を確認できなかった（家庭内の無線装置であることが確認できなかった）ことを接続要求応答部102へ出力する。すると接続要求応答部102は、接続要求を受理できなかったことを示す接続要求受理信号を無線通信部101を介して他の無線装置へ出力する。

【0030】鍵情報管理部105は、接続要求応答部102が接続要求を受理した場合、暗号化・復号化部107で管理していた鍵情報を、第2通信部106を介して前記接続要求を出した他の無線装置へ出力する。また、鍵情報管理部105は、接続要求応答部102が接続要求を受理しなかった場合、暗号化・復号化部107で管理していた鍵情報を、第2通信部106を介して前記接続要求を出した他の無線装置へは出力しない。

【0031】暗号化・復号化部107は、鍵情報管理部105から鍵情報が入力されるとデータ処理部108からの送信データを暗号化して無線通信部101に出力する。また暗号化・復号化部107は無線通信部101で受信した暗号化データを復号化してデータ処理部108に出力する。しかし、鍵情報管理部105から鍵情報が入力されない場合には、暗号化・復号化処理は行わない。

【0032】このようにして接続要求を出した他の無線装置が正しい無線装置（家庭内の無線装置）の場合通信が行われ、正しくない無線装置（家庭内の無線装置でない）の場合通信が行われない。

【0033】（接続要求をする無線装置の構成）図1は接続要求に応答する無線装置であったが、次に接続要求

をする側の無線装置について図2を用いて詳細に説明する。

【0034】図2は、本発明に係る接続要求をする無線装置の構成を説明するためのブロック図である。

【0035】この無線装置は家庭内に置かれた他の無線装置に対して接続要求を行い、自機が家庭内の無線装置からの接続であるかの確認の問い合わせに適切に回答して接続を確立する。

【0036】まず、無線装置200の構成について説明する。

【0037】図2に示すように、無線装置200は、他の機器と無線により通信を行う無線通信部201、他の無線装置に対して接続要求する接続要求部202、自機が他の無線装置と同じ家庭内に存在するか否かの確認に回答する無線装置存在確認応答部203、無線通信部201を介して他の無線装置からの正当性確認に回答する正当性確認応答部204、スクランブルに用いる鍵情報を管理する鍵情報管理部205、無線通信部201とは別の系（例えば有線）で通信を行う第2通信部206、通信するデータを暗号化・復号化する暗号化・復号化部207、通信するデータを送受処理するデータ処理部208から構成されている。

【0038】次に、このように構成された無線装置200の動作について詳細に説明する。

【0039】接続要求送信部202は、無線通信部201を介して他の無線装置に対して接続要求を送信する。この接続要求を受けた他の無線装置は、当該他の無線装置内の第2通信部106を介して図1で説明した通り存在確認を行うことになる。この存在確認時、無線装置存在確認応答部203は、第2通信部206を介して他の無線装置と通信を行い存在確認に正しく応答する。この応答後、他の無線装置から第2通信部206を介して鍵情報が入力されるので、鍵情報管理部205はこの鍵情報を管理する。

【0040】鍵情報管理部205は、管理する鍵情報を正当性確認応答部204に出力する。この鍵情報が正当性確認応答部204に入力された後、他の無線装置は無線通信部201を介して正当性確認を行うことになる。この正当性確認時、正当性確認応答部204は、無線通信部201を介して他の無線装置と通信を行い、図1で説明した通り正当性の確認を行う。

【0041】この正当性の確認後、接続要求部202は他の無線装置から無線通信部201を介して接続要求受理を受け取る。接続要求部202が接続要求受理を受け取ると、鍵情報管理部205は管理している鍵情報を暗号化・復号化部207に出力する。正当性の確認が行われなかった場合には、自機は正しくない無線装置（家庭内の無線装置でない）と接続要求先の他の無線装置に判断されてしまったことになるので通信は行われない。

【0042】暗号化・復号化部207はデータ処理部2

08から入力された送信データを暗号化して無線通信部201を介して他の無線装置に出力する。また暗号化・復号化部207は無線通信部201で受信した暗号化データを復号化してデータ処理部208に出力する。

【0043】このようにして接続要求を受けた他の無線装置が自機を正しい無線装置（家庭内の無線装置）と判断した場合通信が行われ、正しくない無線装置（家庭内の無線装置でない）合通信が行われない。

【0044】次に、本発明に係る無線装置が家庭内でどのように接続されるかについて図3を用いて詳細に説明する。

【0045】図3は、本発明に係る無線装置が家庭内で無線装置の接続を示す図である。この図3では、無線装置Aは図1で説明した接続要求応答する無線装置、無線装置Bおよび無線装置Cは図2を用いて説明した接続要求装置であるものとして説明する。

【0046】無線装置Bは無線装置Aと同一家庭内の装置であり、無線装置Aと問題なくアクセスする権利がある。無線装置Bは無線装置Aに対して無線経路で接続要求を行う。無線装置Aは接続要求を受信すると無線装置Bに対し鍵情報を、例えば電灯線Aを経由して送信すると共に、正当性確認のためのメッセージを無線経路で送信する。無線装置Bは電灯線Aより受信した鍵情報を用いて無線経路で受信したメッセージを暗号化して無線装置Aに返送する。無線装置Aは無線装置Bから届いた暗号化メッセージを電灯線A経路で送付した鍵情報を用いて復号し、送信したメッセージと一致すれば無線装置Bは家庭内の装置であると判断して無線通信を許可する。

【0047】一方、無線装置Cは無線装置Aとは別の家庭内の装置である。この場合、無線装置Aが無線装置Cからの接続要求を許可してしまうと、無線装置Aの持つ情報を無線装置Cが不正に取得できることとなり問題がある。

【0048】無線装置Cが無線装置Aに接続要求を行った場合、無線装置Aは無線装置Bの場合と同様電灯線Aを経由して無線装置Cに鍵情報を伝送しようとする。しかし無線装置Cは隣の家の、電灯線Aとは別の電灯線Bに接続されており、無線装置Cは無線装置Aから鍵情報を受け取ることができない。このため無線装置Aからの正当性確認に応答することができず、無線装置Aは不正アクセスと判断して接続要求を破棄する。

【0049】以上説明したとおり、同一家庭内の装置では接続要求が許可され、同一家庭内に無い装置同士では接続要求が破棄される。

【0050】なお、図3は電灯線で接続されているものとして説明したが、これに限らず有線で通信ができるものであれば何でも良い。

【0051】次に、本発明における無線接続の動作手順について図4を用いて詳細に説明する。

【0052】図4は、本発明における無線接続の動作手

順を示す図である。

【0053】図4において、（手順1）まず無線装置Bから無線装置Aに対し接続要求を送信する。

【0054】（手順2）次に無線装置Aから無線装置Bに対して電灯線（有線）経路で鍵情報（鍵K）を送付する。

【0055】（手順3）無線装置Aは接続要求装置の正当性を確認する。

【0056】（手順4）無線装置Bは正当性確認に応答する。

【0057】（手順5）正当性を確認した無線装置Aは接続要求が受理されたことを無線装置Bに通知し、これによりデータ通信が行われる。

【0058】次に、本発明における無線接続において不正アクセスを排除する場合の動作手順について図5を用いて詳細に説明する。

【0059】図5は、本発明における無線接続において不正アクセスを排除する場合の動作手順を示す図である。図5において、（手順1）まず無線装置Cから無線装置Aに対し接続要求を送信する。

【0060】無線装置Cからの接続要求を受け取った無線装置Aは図4の手順2と同様にして無線装置Cに対して電灯線Aを経由して鍵情報（鍵K）の送付を試みるが、電灯線Aとは別の電灯線Bに接続されているため無線装置Cは無線装置Aから鍵情報を受け取ることができない。このため無線装置Cは無線装置Aからの（手順3）に対して正しい応答（手順4）を返すことが出来ず、（手順5）の接続要求は破棄され、通信することが出来なくなる。

【0061】次に、本発明における携帯型の無線装置における無線接続の動作手順について図6を用いて詳細に説明する。

【0062】図6は携帯型の無線装置における接続方法の概略を示す図である。図6において、モバイルオーディオプレーヤ等の携帯型無線装置の場合、通常は電灯線と切り離し持ち歩いて使う。このため接続要求時に電灯線経路で装置を確認することはできない。

【0063】本発明では携帯型無線装置の場合、図6（a）に示す通り一度目については充電用のアダプタを経由して鍵Kを送付する。そして図6（b）に示す通り2度目以降については携帯無線装置側はメモリ等に図6（a）で保持した鍵情報（鍵K）を無線装置Aからの正当性確認には正しく応答することができる。

【0064】次に、本発明における無線通信手段とは別の通信手段として有線のIEEE1394を適用した場合について図7および図8を用いて詳細に説明する。

【0065】図7および図8は無線通信手段とは別の通信手段として有線のIEEE1394を適用した場合を説明するための図である。図7において、無線装置A、無線装置B、無線装置Cは部屋1に配置されIEEE1

394を介して接続されており、無線装置X、無線装置Y、無線装置Zは部屋2に配置されIEEE1394を介して接続されている。但し部屋1のIEEE1394と部屋2のIEEE1394とは有線では接続されていない。

【0066】従来の方式では、無線装置Aや無線装置X以外に、無線装置Bや無線装置Yなど全ての無線装置に鍵情報を設定しなければ、全ての装置間での無線接続はできなかった。

【0067】本発明によれば、まず無線装置Aおよび無線装置Xは人手による入力やメディア経由等従来の手段を用いて鍵情報の交換を行う。この際無線装置AはIEEE1394接続された無線装置Bおよび無線装置Cに対してもIEEE1394経由で鍵情報を伝送する。同様に無線装置Xは無線装置Yおよび無線装置Zに鍵情報を伝送する。

【0068】これにより無線装置Aおよび無線装置Xだけ設定することにより、IEEE1394接続されたこの家庭内全ての装置の無線設定を完了することが出来る。

【0069】次にこの無線設定後、部屋1と部屋2間で図8に示す通り無線装置を入れ替えた場合の従来の技術と本発明との違いについて説明する。図8は、無線装置Bおよび無線装置Cが部屋1から部屋2へ移動して有線のIEEE1394ネットワークに接続され、無線装置Xおよび無線装置Zが部屋2から部屋1へ移動して有線のIEEE1394ネットワークに接続された点が図7と比べて変更されている。

【0070】例えば無線装置Aと無線装置Bとの無線接続について考える。

【0071】従来の方式では、レイアウト変更前には無線装置Aと無線装置Xとの無線接続設定しか行っておらず、レイアウト変更により別の部屋に切り離されてしまった無線装置Aと無線装置Bに対して新たに設定を行う必要があった。

【0072】本発明によれば、無線装置Aと無線装置Bは有線IEEE1394で接続されていた時に、有線IEEE1394経由で無線装置Aと無線装置Y間で行われた無線接続の設定を無線装置Bにも反映させるため、後日有線接続されていない別の部屋に移動した場合でも、無線装置Aと無線装置Bに対して新たに設定することなく無線装置Aと無線装置B間で無線通信を行うことができる。

【0073】このように図8に示す通りレイアウト変更したとしても、図7で接続したときにメモリ等に保持している鍵情報を用いることにより、IEEE1394接続時に行った事前の設定により無線通信を開始することができる。

【0074】次に、本発明における正当性確認の具体例について図9を用いて詳細に説明する。

【0075】図9は、接続要求に応答する無線装置と、接続要求する無線装置との間で、装置の正当性を確認する一例を示す図である。ここでは一般的な2パス相手認証による正当性確認の例を示す。認証方法は他にも種々考えられ、本発明はいずれを適用しても良い。正当性の確認は接続要求する無線装置が接続要求に応答する無線装置と同じ鍵情報を保持しているから正当性を判断することができる。同一家庭内の無線装置であれば電灯線等の有線経由で鍵情報を正しく伝送できるので、鍵情報を保有していれば同一家庭内の無線装置と判断することが出来る。

【0076】次に正当性確認の手順について説明する。接続要求に応答する無線装置Bは（手順1）まず乱数Raを発生する。

【0077】（手順2）次に接続要求に応答する無線装置Bがこの発生した乱数Raを接続要求する無線装置Aに送付する。

【0078】（手順3）接続要求する無線装置Aは、乱数Raを、メモリ等に保有している鍵情報である鍵Kで暗号化する。

【0079】（手順4）接続要求する無線装置Aは、接続要求に応答する無線装置Bに返送する。

【0080】（手順5）接続要求に応答する無線装置Bは、受信した暗号化鍵K(Ra)を鍵情報である鍵Kで復号化して、もともと保持していた乱数Raと比較する。接続要求する無線装置Aから送られてきた乱数Ra'が（手順2）で発生した乱数Raと一致すれば、接続要求する装置Aは鍵情報である鍵Kを保持していると判断することができ、同一家庭内の正当なアクセス権をもつ装置と判断することができる。

【0081】次に、本発明における無線装置の接続要求時に接続要求装置から伝送される装置識別IDについて図10を用いて詳細に説明する。

【0082】図10は、接続要求時に接続要求装置から伝送される装置識別IDの具体例を示す図である。図10(a)に示すエコーネットアドレスは、電灯線を含む家庭内ネットワークの規格であるエコーネットで用いられるアドレスであり、8bitのNetID（ネットID）と8bitのNodeID（ノードID）からなる。図10(b)に示すIEEE1394アドレスは、IEEE1394での通信に用いるアドレスであり、10bitのBusID（バスID）と6bitのNodeID（ノードID）からなる。接続要求する装置から接続要求に応答する無線装置は、このアドレス情報の示す無線装置に鍵情報を伝送する。

【0083】次に、本発明における接続要求に応答する無線装置Bにおける接続要求応答時の動作について図11を用いて詳細に説明する。

【0084】図11は、本発明における接続要求に応答する無線装置Bにおける接続要求に応答するときの動作

を示すフローチャートである。図11において、接続要求に応答する無線装置Bは、接続要求する無線装置Aから接続要求を受信する(ステップ1101)。次に、接続要求に応答する無線装置Bは、接続要求する無線装置Aが既に鍵情報を保持しているかを確認する(ステップ1102)。

【0085】接続要求に応答する無線装置Bは、ステップ1102において、接続要求する無線装置Aが鍵情報を保持していない場合鍵情報を発生させ(ステップ1103)、ステップ1104へ進む。また、接続要求に応答する無線装置Bは、ステップ1102において、接続要求する無線装置Aが鍵情報を保持している場合にはステップ1104へ進む。

【0086】接続要求に応答する無線装置Bは、ステップ1104では、鍵情報を有線の通信手段を経由して接続要求する装置に送付する。

【0087】次に、接続要求に応答する無線装置Bは乱数を発生し(ステップ1105)、この発生した乱数を無線の通信手段を経由して接続要求する無線装置Aに送付する(ステップ1106)。

【0088】接続要求する無線装置Aは、接続要求に応答する無線装置Bから暗号化された乱数を無線の通信手段を経由して受信し、これを鍵情報を用いて暗号化した後、接続要求に応答する無線装置Bへ送り返す。

【0089】接続要求に応答する無線装置Bは、接続要求する無線装置Aから暗号化された乱数を受信し、この暗号化された乱数を復号化する(ステップ1108)。

【0090】接続要求に応答する無線装置Bは、ステップ1108で復号化した乱数と、ステップ1105で発生した乱数とが一致するかどうかを判定する(ステップ1109)。

【0091】接続要求に応答する無線装置Bは、ステップ1109の判定の結果、一致する場合には接続要求を受信し(ステップ1110)、無線通信を開始する(ステップ1111)。反対に、ステップ1109の判定の結果、一致しない場合には接続要求を破棄する(ステップ1112)。

【0092】次に、本発明における接続要求する無線装置Aにおける接続要求時の動作について図12を用いて詳細に説明する。

【0093】図12は、本発明における接続要求する無線装置Aにおける接続要求するときの動作を示すフローチャートである。図12において、接続要求する無線装置Aは、接続要求に応答する無線装置Bに対し接続要求を行う(ステップ1201)。

【0094】次に接続要求する無線装置Aは、接続要求に応答する無線装置Bから有線の通信手段を経由して鍵情報を受信する(ステップ1202)。

【0095】次に接続要求する無線装置Aは、無線手段を経由して乱数を受信する(ステップ1203)。

【0096】次に接続要求する無線装置Aは、ステップ1203で受信した乱数を鍵情報で暗号化する(ステップ1204)。

【0097】次に接続要求する無線装置Aは、ステップ1204で暗号化した鍵情報を接続要求に応答する無線装置Bに送付する(ステップ1205)。

【0098】次に接続要求する無線装置Aは、接続要求に応答する無線装置Bで接続が受理された場合、接続要求が受理されたことを示す応答が返るので、これを受信し(ステップ1206)、接続要求に応答する無線装置Bと無線通信を開始する(ステップ1207)。

【0099】なお、本発明の有線通信装置が電灯線に接続されている場合には、この電灯線は家庭内の別の電灯線に情報を転送するブレーカ装置を含むことにより、電灯線がブレーカをはさんで複数の系統に分割されている場合でも、家庭内の装置を正しく判別することができる。

【0100】また、装置を識別するための情報は、無線通信のための設定情報とすることにより、接続要求する装置側に無線のための詳細な設定を省略することができる。

【0101】

【発明の効果】以上説明したようにこの発明によれば、無線経由で接続要求を行った装置が正当なアクセス権を持つ装置であるかを、同一家庭内のみで終結する第2の通信手段経由で確認しているので、人手による設定を行わずに隣接した家等外部からの不正な接続要求を排除し、同一家庭内の装置のみの安全な無線通信ネットワークを構築することができる。

【図面の簡単な説明】

【図1】本発明に係る接続要求に応答する無線装置の構成を説明するためのブロック図。

【図2】本発明に係る接続要求をする無線装置の構成を説明するためのブロック図。

【図3】本発明に係る無線装置が家庭内で無線装置の接続を示す図。

【図4】本発明における無線接続の動作手順を示す図。

【図5】本発明における無線接続において不正アクセスを排除する場合の動作手順を示す図。

【図6】携帯型の無線装置における接続方法の概略を示す図。

【図7】無線通信手段とは別の通信手段として有線のIEEE1394を適用した場合を説明するための図。

【図8】無線通信手段とは別の通信手段として有線のIEEE1394を適用した場合を説明するための図。

【図9】接続要求に応答する無線装置と、接続要求する無線装置との間で、装置の正当性を確認する一例を示す図。

【図10】接続要求時に接続要求装置から伝送される装置識別IDの具体例を示す図。

15

【図11】本発明における接続要求に回答する無線装置Bにおける接続要求に回答するときの動作を示すフローチャート。

【図12】本発明における接続要求する無線装置Aにおける接続要求するときの動作を示すフローチャート。

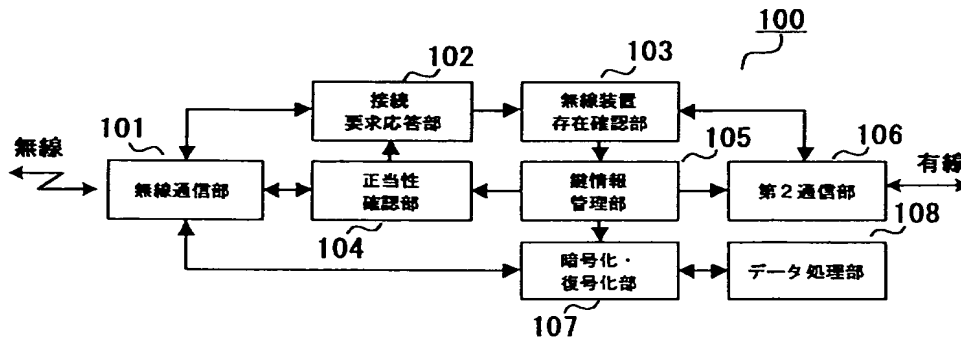
【符号の説明】

100、200…無線装置、101、201…無線通信

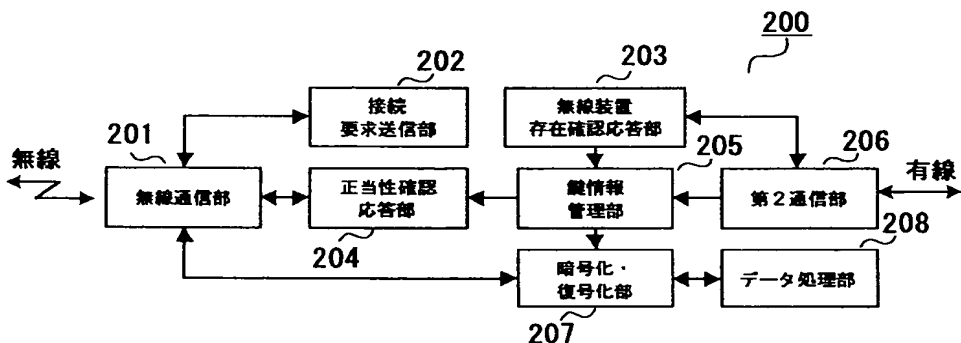
16

部、102…接続要求応答部、103…無線装置存在確認部、104…正当性確認部、105、205…鍵情報管理部、106、206…第2通信部、107、207…暗号化・復号化部、108、208…データ処理部、202…接続要求送信部、203…無線装置存在確認応答部、204…正当性確認応答部。

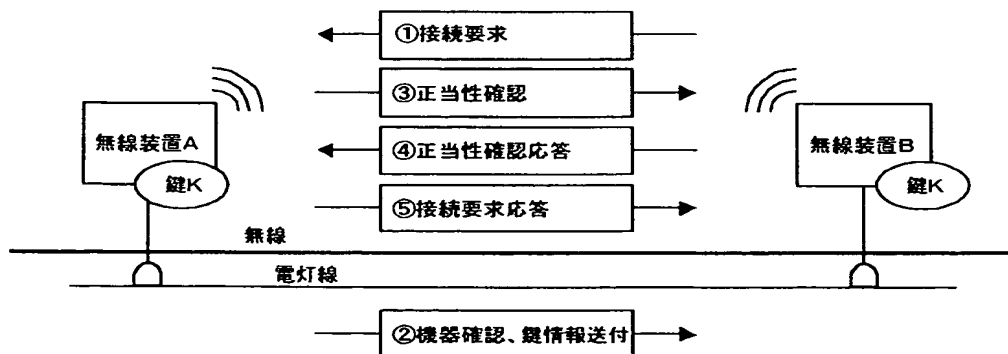
【図1】



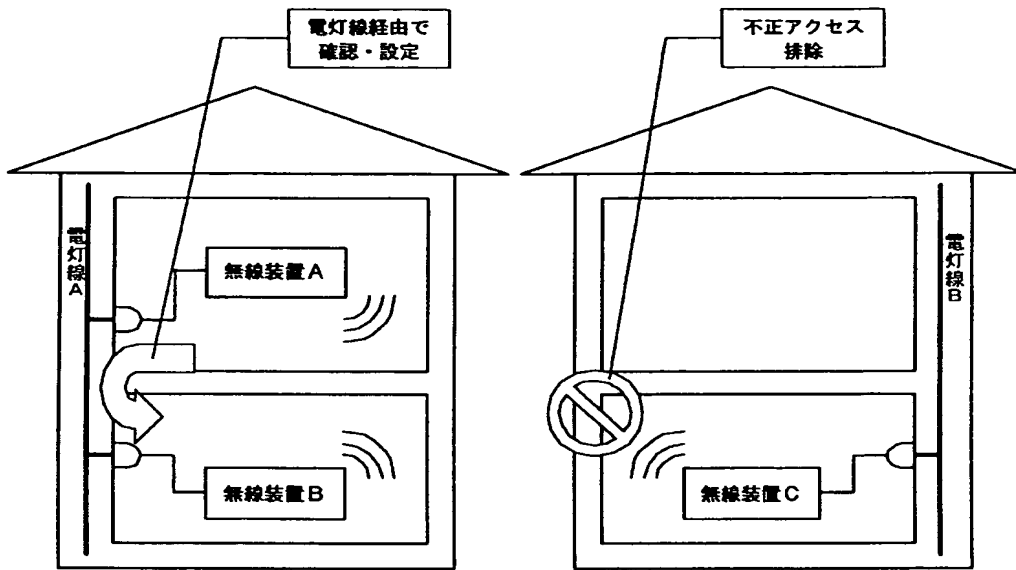
【図2】



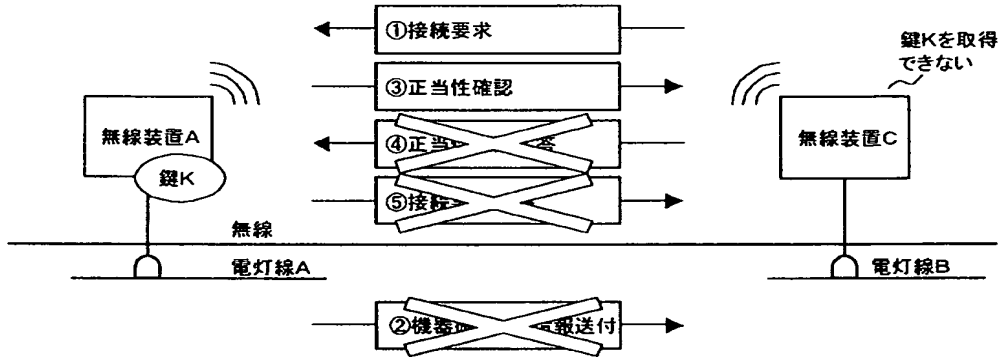
【図4】



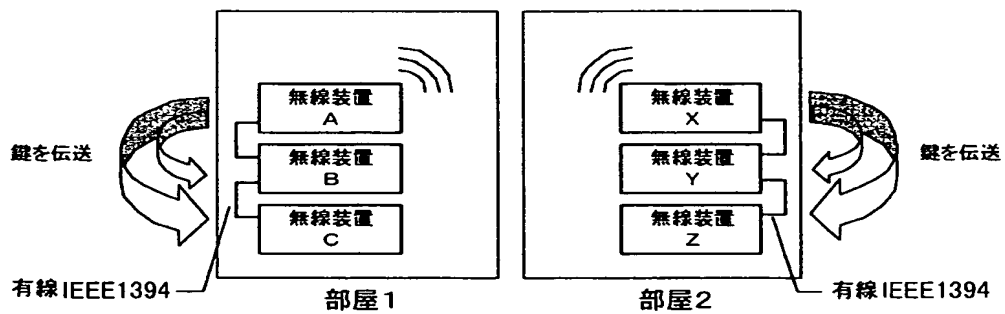
【図3】



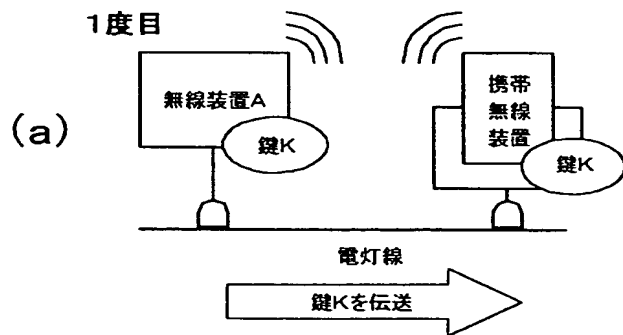
【図5】



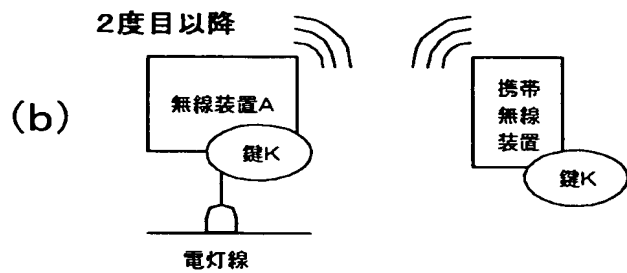
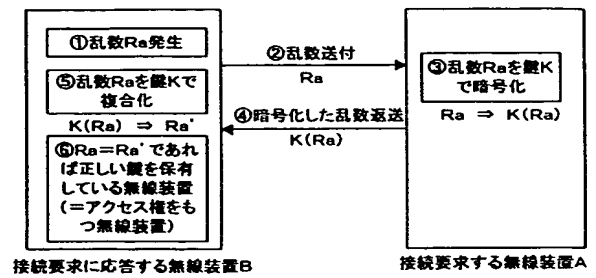
【図7】



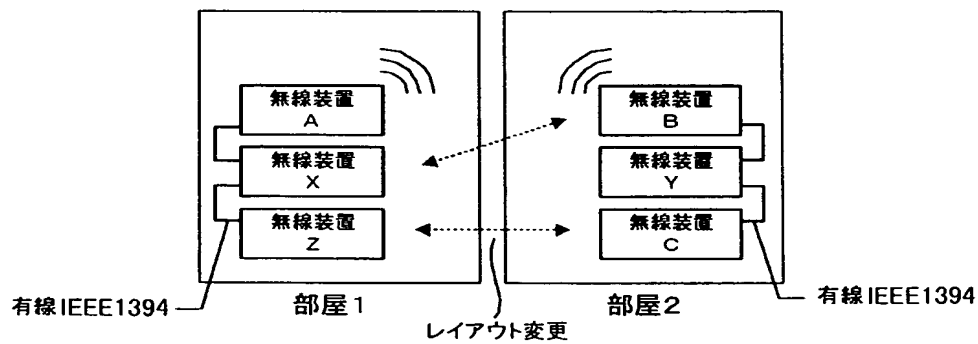
【図6】



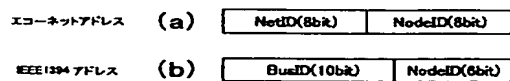
【図9】



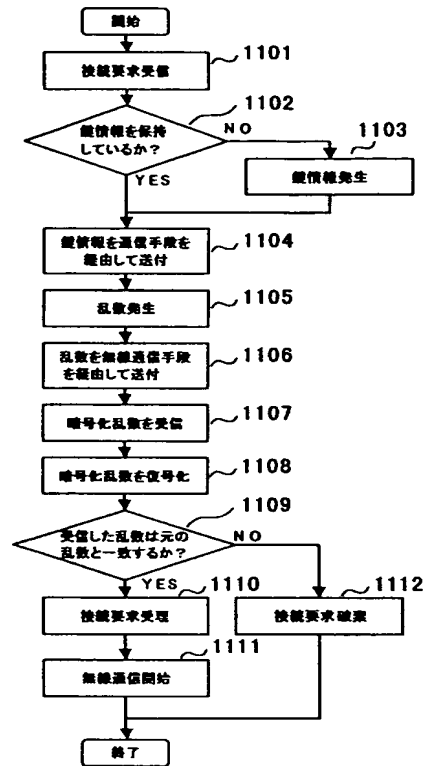
【図8】



【図10】



【図11】



フロントページの続き

(51) Int. Cl. 7

H 0 4 L 12/40

識別記号

F I

H 0 4 L 9/00

テームコード (参考)

6 0 1 E

6 5 1

(72) 発明者 茶木 宏之

神奈川県横浜市磯子区新杉田町 8 番地 株

式会社東芝横浜事業所内

F ターム (参考)

5J104 AA15 AA16 EA04 EA16 EA24

NA02

5K032 AA08 BA01 DA02 DA20

5K033 AA08 BA01 CB01 DA02 DA13

DA17 DB23

5K046 AA03 PS43